NATO
NORTH ATLANTIC TREATY ORGANIZATION
INTERNATIONAL STAFF

OTAN
ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD
SECRÉTARIAT INTERNATIONAL

VACANCY NOTIFICATION/ NOTIFICATION DE LA VACANCE DU POSTE

Officer, Cyber Security and Audit (220446)

Primary Location Belgium-Brussels
NATO Body NATO International Staff (NATO IS)
Schedule Full-time
Application Deadline 10-Jul-2022
Salary (Pay Basis) 5,735.66Euro (EUR) Monthly
Grade NATO Grade G15-G17
Clearance Level CTS

Description

1. SUMMARY

The Joint Intelligence and Security Division (JISD) Division, under the leadership of the Assistant Secretary General (ASG) for Intelligence and Security, comprises two principal pillars: Intelligence, headed by the Deputy ASG for Intelligence; and the NATO Office of Security (NOS), headed by the Deputy ASG for Security.

The NOS is responsible for the overall coordination of NATO security among member Nations, NATO civil and military bodies as well as International Organisations and partner countries with which NATO cooperates. It is also responsible for the security of the NATO Headquarters and its personnel in Brussels and abroad on mission and in satellite offices, and for the protection of the Secretary General. The NOS comprises the Office of the Director, the Security and Policy Oversight Branch (SPOB), the Protective Security and Emergency Services Branch, the Security Intelligence Branch and the Close Protection Unit.

The SPOB is responsible for ensuring that NATO Security Policy is applied throughout NATO bodies and member Nations, as well as in non-NATO nations and international organisations with whom NATO cooperates. SPOB develops security policy, directives and guidance documents, supports their implementation and verifies compliance through security audits in the specific functional areas of personnel security, physical security, security of information, communication and information systems security (including Cyber Security), industrial and protective security. SPOB works with the other NOS branches to ensure coordinated and consistent responses to the interpretation and practical application of policy.

Across the NATO Headquarters, the incumbent is responsible for ensuring the appropriate mitigation of insider threat (including cyber) against NATO Communication and Information Systems (CIS) and other electronic systems or the information that is stored, processed or transmitted in these systems. S/he is responsible for performing continuous monitoring and user behaviour auditing to identify suspicious or disruptive behaviour, or evidence of the presence of

insider threat actors, to NATO classified systems. S/he will perform log correlation and auditing of staff and business partners' suspicious activities, to establish a baseline of normal user behaviour when interacting with NATO classified systems.). The incumbent supports the role of Security Accreditation Authority assumed by the NOS for the NATO Headquarters. Furthermore, the incumbent will contribute to JISD's cyber situational awareness and security risk management activities in particular identifying and evaluate the risks to the users, projects and business and recommending safeguards to control risks.

2. QUALIFICATIONS AND EXPERIENCE

ESSENTIAL

The incumbent must:

- possess a university degree, preferably in the field of CIS engineering, computer science or similar;
- possess at least 4 years of professional working experience in Information Assurance, CIS/Cyber Security or in CIS auditing activities, dealing with CIS/Cyber Security incident handling and investigations;
- possess recent experience within the last years, performing cyber incident investigation and coordination, or post-incident analysis in environments with high security requirements similar to NATO;
- possess effective interpersonal skills in performing investigative interviews;
- possess advanced knowledge and application of the Security Policy and subordinate Directives in national or international environments;
- possess knowledge in the area of investigation methodologies, digital forensics, incident response, breach indicator and analysis, data leakage and data theft, cyber espionage, cyber incident legal matters and privacy concerns;
- demonstrate in-depth understanding of the methods used to both compromise and defend modern CIS infrastructures, a good understanding of the current cyber threats and knowledge of hacker capabilities and techniques;
- demonstrate excellent oral and written reporting and presentation skills;
- possess the following minimum levels of NATO's official languages (English/French): V ("Advanced") in one; I ("Beginner") in the other.

DESIRABLE

The following would be an advantage:

- a higher university degree (master or Ph.D.) related to IT, security and/or professional security certification credentials (such as Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), or EnCase Certified Examiner (EnCE));
- practical experience of commercial Security Information and Event Management tools (i.e. Splunk);
- familiarity in conducting insider and cyber threat analysis including online monitoring of user behavior in the IT environment and advanced knowledge on insider threat mitigation strategies and techniques;
- possess advanced knowledge of the Security Policy, Directives and Regulations of NATO project management skills (i.e. PRINCE2);
- experience in conducting or managing digital Forensics;
- familiarity with SharePoint technologies, workflows and data driven solutions;
- experience in supervising the installation, configuration and maintenance of software within a

classified environment.

3. MAIN ACCOUNTABILITIES

Project Management
Perform the planning and implementation of NATO HQ insider threat mitigation programme. Ensure that the programme and its activities contribute to the Organisation mission and reflect the priorities of its leadership. Lead and monitor special projects related to user behaviour auditing and investigations. Work closely with project and programme managers to consistently enforce policies and controls. Define explicit auditing requirements. Institute appropriate access controls and monitoring policies on specific user's categories (i.e. remote users, etc.).

Policy Development
Support the HQ CIS Security Regulations and policy development in her/his field of expertise. Ensure compliance with NATO Security Policy requirements on security incident investigation and reporting. Assure the consistent classification of incidents and the remediation and mitigation of critical incidents are comparable across the Organization.

Stakeholder Management
Serve as the primary point of contact within NOS/SPOB for user behaviour auditing. Is eligible to exercise the role of NATO HQ Communication and Information System Security Officer (HQ CISSO). Ensure collaboration with NATO HQ security, counter intelligence and cyber defence staff. Assist in the management of the section resources related to continuous monitoring, auditing and digital investigation activities, provide technical expertise and ensure their effective coordination. Establish and maintain working relations with the NATO-wide CIS Security Officers and Counter Intelligence community, local security authorities and collaboration with human resources, counter-intelligence, cyber defence and security investigations staff. Deputize the Head Cyber Investigation and Auditing section and provide support to section's activities.

Expertise Development
Perform both continuous monitoring and user behaviour auditing activities. Develop scenarios, integrate structure and unstructured data and apply correlation rules for generating alerts on suspicious or abnormal activities. Review and adjust associated triggers for continuously improving the detection capabilities. Expand knowledge and experience in the use and application of analytical tools relevant to user behaviour auditing, big data analysis and digital investigations such as computer and network Forensics. Adapt to changing work methods and show an active interest in future developments in the field. Assist in designing and updating existing security mechanisms and requirements for improving the Organisation's insider threat prevention and detection capabilities. Incorporate insider threat awareness into periodic security training of all employees. Be vigilant regarding proper usage of social media.

Financial Management
Plan, coordinate and monitor the allocated financial resources in terms of budget, and training including outsourced contracts in an efficient manner, to accomplish the objectives and enhance the operational effectiveness of the section.

Planning and Execution
Develop and maintain the appropriate methodologies and procedures for insider threat mitigation programme. Conduct and synthesise trend analysis from related information sources.

Knowledge Management
Know the available assets. Establish and maintain baselines of device and user behaviour. Anticipate and manage foreseeable insider threats from malicious actors. Share expertise, lessons learned and best practices with others.
Perform any other related duty as assigned.

4. INTERRELATIONSHIPS

The incumbent reports to the Section Head of Cyber Investigation and Auditing. S/he will maintain regular contact with the section heads within SPOB as well as other across the Division as required. S/he will work closely with Divisional Security Officers, Cyber Security and security management staff in other Divisions. S/he liaises closely with CIS Security Officers, Incident Responders and Counter-Intelligence NATO-wide staff, and any NATO staff who contribute managing the insider threat. S/he will contribute as a SPOB team member in the investigation of the CIS/Cyber Security Incidents and cyber awareness material as directed by the head of section.
Direct reports: N/a
Indirect reports: N/a.

5. COMPETENCIES

The incumbent must demonstrate:
- Analytical Thinking: Sees multiple relationships;
- Flexibility: Adapts to unforeseen situations;
- Impact and Influence: Takes multiple actions to persuade;
- Initiative: Is decisive in a time-sensitive situation;
- Organisational Awareness: Understands organisational climate and culture;
- Teamwork: Cooperate.

6. CONTRACT

Contract to be offered to the successful applicant (if non-seconded): Definite duration contract of three years; possibility of renewal for up to three years, during which the incumbent may apply for conversion to an indefinite duration contract.

Contract clause applicable:

In accordance with the contract policy, this is a post in which turnover is desirable for political reasons in order to be able to accommodate the Organisation's need to carry out its tasks as mandated by the Nations in a changing environment, for example by maintaining the flexibility necessary to shape the Organisation's skills profile, and to ensure appropriate international diversity.

The maximum period of service foreseen in this post is 6 years. The successful applicant will be offered a 3-year definite duration contract, which may be renewed for a further period of up to 3 years. However, according to the procedure described in the contract policy the incumbent may

apply for conversion to an indefinite contract during the period of renewal and no later than one year before the end of contract.

If the successful applicant is seconded from the national administration of one of NATO's member States, a 3-year definite duration contract will be offered, which may be renewed for a further period of up to 3 years subject also to the agreement of the national authority concerned. The maximum period of service in the post as a seconded staff member is six years.

Serving staff will be offered a contract in accordance with the NATO Civilian Personnel Régulations.

NOTE: Irrespective of previous qualifications and experience, candidates for twin-graded posts will be appointed at the lower grade. Advancement to the higher grade is not automatic, and will not normally take place during the first three years of service in the post.

Under specific circumstances, serving staff members may be appointed directly to the higher grade, and a period of three years might be reduced by up to twenty four months for external candidates. These circumstances are described in the IS directive on twin-graded posts.

7. RECRUITMENT PROCESS

Please note that we can only accept applications from nationals of NATO member countries.

Applications must be submitted using e-recruitment system, as applicable:

- For NATO civilian staff members only: please apply via the internal recruitment portal (link);
- For all other applications: www.nato.int/recruitment

Please note that at the time of the interviews, candidates will be asked to provide evidence of their education and professional experience as relevant for this vacancy.

Appointment will be subject to receipt of a security clearance (provided by the national Authorities of the selected candidate) and approval of the candidate's medical file by the NATO Medical Adviser.

More information about the recruitment process and conditions of employment, can be found at our website (http://www.nato.int/cps/en/natolive/recruit-hq-e.htm).

8. ADDITIONAL INFORMATION

NATO is committed to diversity and inclusion, and strives to provide equal access to employment, advancement and retention, independent of gender, age, nationality, ethnic origin, religion or belief, cultural background, sexual orientation, and disability. NATO welcomes applications of nationals from all member Nations, and strongly encourages women to apply.

Building Integrity is a key element of NATO's core tasks. As an employer, NATO values commitment to the principles of integrity, transparency and accountability in accordance with international norms and practices established for the defence and related security sector. Selected candidates are expected to be role models of integrity, and to promote good governance through ongoing efforts in their work.

Due to the broad interest in NATO and the large number of potential candidates, telephone or e-mail enquiries cannot be dealt with.

Applicants who are not successful in this competition may be offered an appointment to another post of a similar nature, albeit at the same or a lower grade, provided they meet the necessary requirements.

The nature of this position may require the staff member at times to be called upon to travel for work and/or to work outside normal office hours.

The organization offers several work-life policies including Teleworking and Flexible Working arrangements (Flexitime) subject to business requirements.

Please note that the International Staff at NATO Headquarters in Brussels, Belgium is a non-smoking environment.

For information about the NATO Single Salary Scale (Grading, Allowances, etc.) please visit our website. Detailed data is available under the Salary and Benefits tab.

Administratrice/Administrateur (cybersécurité et audit) (220446)

Emplacement principal Belgique-Bruxelles
Organisation OTAN SI
Horaire Temps plein
Date de retrait 10-juil.-2022
Salaire (Base de paie) 5 735,66Euro (EUR) Mensuelle
Grade NATO Grade G15-G17
Niveau de l'habilitation de sécurité CTS

Description

1. RÉSUMÉ

La Division civilo-militaire Renseignement et sécurité (JISD), placée sous l'autorité de la/du secrétaire général(e) adjoint(e) (ASG) pour le renseignement et la sécurité, se compose de deux grands piliers : le pilier « renseignement », dirigé par la/le secrétaire général(e) adjoint(e) délégué(e) pour le renseignement (DASG/I), et le pilier « sécurité », à savoir le Bureau de sécurité de l'OTAN (NOS), dirigé par la/le secrétaire général(e) adjoint(e) délégué(e) pour la sécurité (DASG/S).

Le NOS est responsable de la coordination générale de la sécurité à l'OTAN entre pays membres et organismes civils et militaires de l'OTAN, ainsi qu'avec les organisations internationales et les pays partenaires avec lesquels l'OTAN coopère. Il est également chargé de la sécurité du siège de l'OTAN et de son personnel à Bruxelles et à l'étranger, en mission et dans les bureaux satellites, et de la protection de la/du secrétaire général(e). Le NOS comprend le Bureau de la directrice/du directeur, la Branche Supervision de la politique et de la sécurité (SPOB), la Branche Sécurité de protection et services de secours (PSESB), la Branche Renseignement de sécurité (SIB) et l'Équipe Protection rapprochée (CPU).

La SPOB veille à ce que la politique de sécurité de l'OTAN soit appliquée dans l'ensemble des organismes et des pays de l'OTAN, ainsi que dans les pays non OTAN et les organisations internationales avec lesquels l'OTAN coopère. Elle élabore la politique de sécurité, ainsi que des directives et des documents d'orientation. Elle appuie leur mise en application et vérifie leur respect au travers d'audits de sécurité dans les domaines fonctionnels spécifiques que sont la sécurité concernant le personnel, la sécurité physique, la sécurité des informations, la sécurité des systèmes d'information et de communication (y compris la cybersécurité), la sécurité industrielle et la sécurité de protection. Elle collabore avec les autres branches du NOS afin de garantir que des réponses coordonnées et cohérentes sont apportées à l'interprétation et à l'application pratique de la politique de sécurité.

La/Le titulaire est responsable, pour l'ensemble du siège de l'OTAN, des mesures d'atténuation des risques de menace interne (menace cyber incluse) contre les systèmes d'information et de communication (SIC) de l'OTAN et les autres systèmes électroniques, et contre les informations stockées, traitées ou transmises dans ces systèmes. Elle/Il assure une surveillance continue des réseaux et étudie le comportement des utilisateurs afin de repérer toute activité suspecte ou perturbatrice ou tout signe de présence d'acteurs malveillants internes sur les systèmes classifiés de l'OTAN. Elle/Il effectue la corrélation des journaux et l'audit des activités suspectes émanant des personnels et des partenaires métiers pour établir une base de référence du comportement

utilisateur standard lorsqu'une personne travaille sur les systèmes classifiés de l'OTAN. La/Le titulaire apporte en outre son concours au NOS dans ses activités d'autorité d'homologation de sécurité pour le siège de l'Organisation. Elle/Il contribue par ailleurs aux activités menées au niveau de la JISD dans le cadre de la connaissance de la situation cyber et de la gestion des risques de sécurité, plus particulièrement à l'identification et à l'évaluation des risques pour les utilisateurs, les projets et les activités, ainsi qu'à la formulation des mesures de protection recommandées pour maîtriser les risques.

2. QUALIFICATIONS ET EXPÉRIENCE

ACQUIS ESSENTIELS

La/La titulaire du poste doit:

- être titulaire d'un diplôme universitaire, de préférence dans le domaine de l'ingénierie des SIC, de l'informatique ou dans un domaine similaire;
- avoir au moins 4 années d'expérience professionnelle dans le domaine de l'assurance de l'information, de la sécurité des SIC, de la cybersécurité, ou de l'audit des SIC axée sur le traitement des incidents de sécurité SIC/cyber et les enquêtes à mener;
- avoir une expérience récente de la conduite et de la coordination d'enquêtes sur des cyberincidents ou d'analyses post-incident dans des environnements hautement sécurisés similaires à l'OTAN;
- avoir de réelles aptitudes relationnelles pour la conduite d'entrevues dans le cadre des enquêtes;
- avoir une connaissance approfondie des politiques de sécurité et des directives subordonnées mises en application dans des environnements nationaux ou internationaux;
- avoir des connaissances dans les domaines suivants : méthodes d'enquête, criminalistique informatique, réponse aux incidents, signalement et analyse des infractions, fuites et vols de données, cyberespionnage, aspects juridiques liés aux cyberincidents et questions liées à la vie privée;
- justifier d'une connaissance approfondie des méthodes utilisées tant pour compromettre que pour défendre des infrastructures SIC modernes, d'une bonne compréhension des cybermenaces actuelles, et d'une connaissance des capacités et des techniques des hackers;
- justifier d'excellentes aptitudes à la rédaction de rapports écrits/verbaux et à la présentation d'exposés;
- avoir au minimum le niveau de compétence V (« avancé » dans l'une des deux langues officielles de l'OTAN (anglais/français) et le niveau I (« débutant ») dans l'autre.

ACQUIS SOUHAITABLES

Seraient considérées comme autant d'atouts:

- la possession d'un diplôme universitaire de plus haut niveau (master ou doctorat) dans un domaine lié à la sécurité ou à l'informatique et/ou d'une certification professionnelle en sécurité informatique comme la certification CISSP (Certified Information Systems Security Professional), CISA (Certified Information Systems Auditor) ou EnCE (EnCase Certified Examiner);
- une expérience pratique d'outils « grand public » de gestion des événements et des informations de sécurité (par exemple Splunk);
- une bonne maîtrise de la conduite d'analyses des menaces internes et cyber, notamment de la surveillance des comportements utilisateurs dans l'environnement informatique, et une connaissance approfondie des stratégies et techniques d'atténuation des menaces internes;

- une connaissance approfondie des politiques, directives et règlements de sécurité à l'OTAN, ainsi qu'une certification en gestion de projet (par exemple PRINCE2);
- une expérience de la conduite d'enquêtes ou de la gestion de dossiers de criminalistique informatique;
- une bonne connaissance de la technologie SharePoint, des solutions de gestion de flux et des solutions orientées données;
- une expérience de la supervision de l'installation, de la configuration et de la maintenance de logiciels dans un environnement classifié.

3. RESPONSABILITÉS PRINCIPALES

Gestion de projet
Planifie et met en œuvre le programme du siège de l'OTAN pour l'atténuation des menaces internes. Veille à ce que ce programme et les activités qu'il comprend contribuent à la mission de l'Organisation et reflètent les priorités de ses dirigeants. Pilote et suit les projets spéciaux d'audit du comportement des utilisateurs et les enquêtes en la matière. Travaille en étroite concertation avec les gestionnaires de projet et de programme pour une mise en application cohérente des politiques et des mesures de contrôle. Définit clairement les besoins en matière d'audit. Établit les politiques de surveillance et les contrôles d'accès nécessaires applicables à certaines catégories d'utilisateurs (par exemple les utilisateurs à distance).

Élaboration des politiques
Contribue aux travaux d'élaboration des politiques et règlements de sécurité des SIC au siège, dans son domaine d'expertise. Veille au respect des exigences de la politique de sécurité de l'OTAN en matière d'enquête sur les incidents de sécurité et de signalement de ceux-ci. Assure un classement cohérent des incidents et veille à ce que les actions correctives et les mesures d'atténuation des incidents critiques soient comparables dans l'ensemble de l'Organisation.

Gestion des parties prenantes
Est le principal point de contact au sein du NOS/SPOB pour les audits de comportement des utilisateurs. Peut être appelé(e) à remplir le rôle d'officier de sécurité des systèmes d'information et de communication du siège de l'OTAN (HQ CISSO). Assure une collaboration avec les services du siège de l'OTAN chargés de la sécurité, de la contre-ingérence et de la cyberdéfense. Apporte son concours à la gestion des ressources dont dispose la Section pour ce qui est des activités de surveillance continue, d'audit et d'investigation numérique ; apporte une expertise technique et assure une coordination efficace. Établit et entretient des relations de travail avec les officiers de sécurité des SIC et la communauté CI (contre-ingérence) à l'échelle de l'OTAN et les autorités de sécurité locales, et collabore avec les services des ressources humaines, de contre-ingérence, de cyberdéfense et d'enquêtes de sécurité. Supplée la/le chef de la Section Enquête et audit cyber et contribue aux activités de la Section.

Développement de l'expertise
Mène à la fois des tâches de surveillance continue et d'audit du comportement des utilisateurs. Conçoit des scénarios, y intègre des données structurées et non structurées, et applique des règles de corrélation pour que des alertes se déclenchent en cas d'activités suspectes ou anormales. Passe en revue et adapte les déclencheurs qui leur sont associés dans une optique d'amélioration continue des capacités de détection. Développe ses connaissances théoriques et pratiques s'agissant de la mise en œuvre des outils adaptés à l'audit de comportement des

utilisateurs, aux analyses big data et aux enquêtes comme les outils de criminalistique informatique machine et réseau. S'adapte aux changements dans les méthodes de travail et porte un vif intérêt aux évolutions intervenant dans son domaine. Aide à concevoir et à actualiser les mécanismes et les prescriptions de sécurité en place afin d'améliorer les capacités dont l'Organisation dispose pour la détection et la prévention des menaces internes. Prévoit un volet sensibilisation à la menace interne dans les formations à la sécurité que tous les employés suivent régulièrement. Fait preuve de vigilance pour ce qui est de la bonne utilisation des réseaux sociaux.

Gestion financière
Planifie, coordonne et contrôle de manière efficace l'emploi des ressources financières allouées (budget et formation, contrats externalisés compris) afin d'atteindre les objectifs de la Section et d'en améliorer l'efficacité opérationnelle.

Planification et exécution
Élabore et tient à jour les méthodes et les procédures destinées au programme d'atténuation de la menace interne. Analyse les tendances à partir de sources d'information pertinentes et en fait la synthèse.

Gestion des connaissances
A connaissance des moyens disponibles. Établit et tient à jour une base de référence des comportements matériel et utilisateur. Anticipe et gère les menaces internes prévisibles émanant d'acteurs malveillants. Fait bénéficier les autres de son expertise, des enseignements tirés et des meilleures pratiques.
S'acquitte de toute autre tâche en rapport avec ses fonctions qui pourrait lui être confiée.

4. STRUCTURE ET LIAISONS

La/Le titulaire du poste relève de la/du chef de la Section Enquête et audit cyber. Elle/Il entretient des contacts réguliers avec les chefs de section de la SPOB ainsi qu'avec les autres composantes de la Division, selon les besoins. Elle/Il collabore étroitement avec les officiers de sécurité de division (DSO) ainsi qu'avec les responsables de la cybersécurité et de la gestion de la sécurité d'autres divisions. Elle/Il se tient en liaison étroite avec les officiers de sécurité des SIC, les équipes d'intervention sur incident et les services chargés de la contre-ingérence dans l'ensemble de l'OTAN, ainsi qu'avec tout agent de l'Organisation contribuant à la gestion de la menace interne. En tant que membre d'une équipe SPOB, elle/il contribue aux enquêtes sur les incidents de sécurité SIC ou cyber et à l'élaboration de supports de sensibilisation à la cybersécurité, selon les instructions de la/du chef de section.
Nombre de subordonné(e)s direct(e)s: sans objet.
Nombre de subordonné(e)s indirect(e)s: sans objet.

5. COMPÉTENCES

La/Le titulaire du poste doit faire preuve des compétences suivantes :

- Réflexion analytique: discerne les relations multiples.
- Flexibilité: s'adapte à des situations imprévues.
- Persuasion et influence: prend différentes mesures à des fins de persuasion.
- Initiative: fait preuve de décision dans les situations où il faut agir sans attendre.
- Compréhension organisationnelle: comprend le climat et la culture de l'Organisation.

- Travail en équipe: Coopère.

6. CONTRAT

Voir la version anglaise.

7. PROCESSUS DE RECRUTEMENT

Voir la version anglaise.

8. INFORMATIONS COMPLÉMENTAIRES

Voir la version anglaise.